# KPN EEN MKB
# Acronis Cyber Protect
Dienstbeschrijving

versie 1.0
December 2021

# Inhoudsopgave

# Inleiding

**Deze dienstbeschrijving geeft u informatie over de clouddienst Acronis Cyber Protect. IT-omgevingen worden in toenemende mate blootgesteld aan cyberdreigingen. Daarom is het absoluut noodzakelijk om hiervoor de juiste beschermingsmaatregelen te treffen. Acronis Cyber Protect is een 2-in-1 cloudoplossing voor cyberbescherming die een gegevensback-up integreert met cyberbeveiliging. Met deze dienst kunt u back-up- en herstelbewerkingen uitvoeren voor fysieke machines (werkstations of servers), virtuele machines en toepassingen zoals Microsoft 365[1].**

U kunt kiezen voor een complete image back-up (een 100% kopie van uw machine, inclusief besturingssysteem en alle geïnstalleerde software) of een bestandsback-up. Ook bij een image back-up kunt u eenvoudig door alle mappen en bestanden bladeren om specifieke mappen of bestanden te herstellen vanuit de back-up.

De gegevens worden via internet versleuteld opgeslagen in Acronis-datacenters in Duitsland. Daarnaast worden alle machines beschermd tegen alle malwarebedreigingen, zoals virussen en ransomware, wordt het downloaden van schadelijke bestanden voorkomen en wordt de toegang tot verdachte webresources geblokkeerd. Ook is het met Acronis Cyber Protect mogelijk om de machine op afstand over te nemen of via een remote desktop client op afstand in te loggen op de machine.

Er zijn twee aanvullende modules bij deze dienst beschikbaar: Advanced Security en Advanced Management. Advanced Security voegt extra veiligheidsfuncties toe en Advanced Management bevat patch-management voor alle applicaties op de machine en een HDD-integriteitscheck.

**De voordelen van Acronis Cyber Protect:**

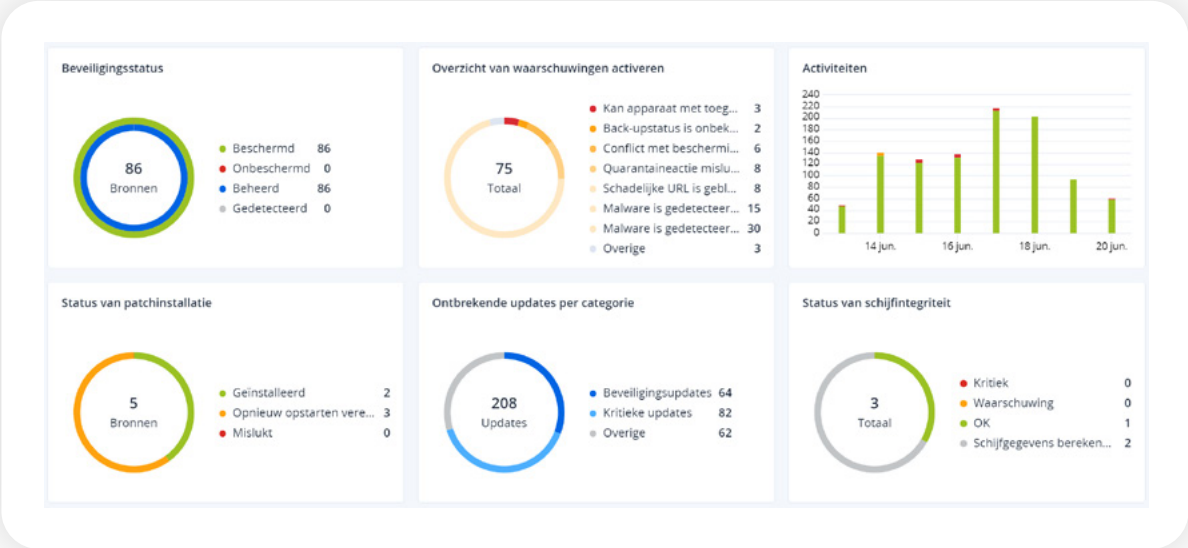
- Maximale veiligheid van uw bedrijfsgegevens.
- Bescherming van uw machines tegen cyberdreigingen, zoals ransomware.
- Automatische image of bestandsback-up.
- Acronis Hosted Cloud Storage bundels van 100 GB tot 5 TB die eenvoudig zowel naar boven als naar beneden aangepast kunnen worden.
- Microsoft 365 back-up met onbeperkte opslagruimte via een losstaande hoofdlicentie.
- Een zeer overzichtelijk dashboard met de status van uw back-up en beveiliging.
- Eenvoudig instellen op welk tijdstip de back-up gemaakt moet worden. Zo vergeet u nooit (meer) om een back-up te maken.
- Geen gedoe met tapes of externe harde schijven. Uw gegevens worden via internet naar het datacenter gestuurd.
- Uw back-up is alleen voor u toegankelijk met een zelfgekozen encryptiesleutel.

Op deze dienst zijn de ‘Algemene Leveringsvoorwaarden’ en ‘Aanvullende Voorwaarden Online Diensten’ van toepassing. U vindt deze op kpn.com/allevoorwaarden bij ‘Zakelijk’ en vervolgens bij ‘Algemene en Aanvullende Voorwaarden’.

[1]Microsoft maakt geen back-up van uw gegevens

# 1 Gebruik van de dienst

Gezien de grote waarde van digitale informatie, is het maken van goede back-ups van essentieel belang voor het borgen van de bedrijfsprocessen binnen uw organisatie. De beschikbaarheid van de belangrijkste data is cruciaal voor uw bedrijfsvoering. Acronis Cyber Protect kan worden gezien als een 'verzekering' voor de opslag van uw belangrijkste data en gegevens. Daarnaast voorziet Acronis Cyber Protect in een optimale cyberbescherming van uw machines (end points) die essentieel is om uw organisatie te beschermen tegen digitale bedreigingen zoals ransomware. Dit levert een mindere belasting op van de machine en een financieel voordeel, omdat aanvullende beveiligingssoftware niet meer noodzakelijk is. Windows Defender kan gemanaged worden vanuit Acronis Cyber Protect. U kunt in 1 overzicht zowel de status van uw back-up als van uw cyberbescherming zien.




## 1.1 Functionaliteiten

De cloudoplossing Acronis Cyber Protect beschikt over uitgebreide back-up- en herstelfuncties voor vrijwel elk besturingssysteem en virtualisatieplatform. Vrijwel alle Windows computer- en serverbesturingssystemen, MacOS-versies, Linux OS-versies en Microsoft 365, Azure, Hyper-V, VMware en Microsoft SQL worden ondersteund. De back-up data worden versleuteld met uw eigen sleutel opgeslagen in Acronis datacenters in Duitsland die beschikken over de hoogste veiligheidscertificeringen zoals SOC-1 en 2, ISO 9001, 27001 en 50001. In hoofdstuk 3 vindt u hiervan een meer gedetailleerd overzicht.

Ook beschikt Acronis Cyber Protect over uitgebreide cyberbeveiligings- en managementfuncties waardoor uw machines beschermd worden tegen cyberdreigingen.

### 1.1.1 Acronis Cyber Protect functiematrix

In onderstaand overzicht worden de belangrijkste standaardfuncties en functies van de additionele modules weergegeven.

| Functiegroep | Inbegrepen in standaardlicentie | Additionele module Advanced Security en/of Advanced Management |
|---|---|---|
| **Security** | • CyberFit-score<br>• Evaluatie van beveiligingsproblemen<br>• Antiransomwarebescherming: Active Protection<br>• Antivirus- en antimalwarebeveiliging: bestandsdetectie in de cloud op basis van handtekeningen (geen real time bescherming, alleen geplande scans)<br>• Antivirus- en antimalwarebeveiliging: op AI gebaseerde bestandsanalyse voorafgaand aan de uitvoering en op gedrag gebaseerd Cyber Engine Microsoft Defender-beheer | • Antivirus- en antimalwarebeveiliging met lokale detectie op basis van handtekeningen (met real time bescherming)<br>• Preventie tegen aanvallen<br>• Url-filtering<br>• Forensische back-up (scannen van back-up op malware, veilig herstel, acceptatielijst van uw organisatie)<br>• Scherma's voor slimme bescherming |
| **Management** | • Groepsbeheer van workloads<br>• Gecentraliseerd beheer van beschermingsschema's<br>• Extern Bureaublad<br>• Hulp op afstand<br>• Hardware-inventaris | • Softwareinventaris<br>• Patchbeheer<br>• HDD-integriteit<br>• Veilige bestandspatches<br>• Cyberscripts<br>• Op AI-gebaseerde controle op software-implementatie |
| **Preventie van gegevensverlies** | • Apparaataansturing<br>• Usb-toegangsbeheer | |
| **Back-up** | • Bestandsback-up<br>• Systeemkopieback-up<br>• Back-up van toepassingen<br>• Back-up naar cloudopslag<br>• Back-up van Office 365, Microsoft 365 (Outlook, SharePoint, OneDrive, Teams) met beperkte cloudopslag | |

Klik hier voor een meer gedetailleerd overzicht.

### 1.1.2 Back-upbeschermingsschema

Het standaard back-upbeschermingsschema dat toegepast wordt is:

- Maandag tot en met vrijdag 10.45 uur. De bewaartijd van deze back-up is 7 dagen.
- Wekelijks. De bewaartijd van deze back-up is 4 weken.
- Maandelijks. De bewaartijd van deze back-up is 6 maanden.

De eerste back-up is een volledige back-up. De overige back-ups zijn incrementele back-ups. U kunt zelf het beschermingsschema (tijdstip van back-up, interval, bewaartijd, type back-up) volledig naar eigen wens aanpassen.

Bij de allereerste back-up wordt de volledige dataset waarvan u een back-up wenst te maken via uw internetverbinding naar de Acronis-datacenters gekopieerd. Hierdoor kan het maken van deze back-up, afhankelijk van de grootte en de upload-snelheid van uw internetverbinding, een uur of langer in beslag nemen. Bij de daaropvolgende back-ups worden alleen de wijzingen in uw dataset verstuurd, waardoor deze back-ups veel sneller te maken zijn.

### 1.1.3 Beveiliging van gegevens

Uw back-upgegevens worden op basis van het cryptografische AES-algoritme en een alleen bij u bekend wachtwoord versleuteld opgeslagen. Hierdoor zijn de back-updata niet voor derden toegankelijk.

**Belangrijk: er is geen manier om versleutelde back-ups te herstellen als u het wachtwoord verliest of vergeet. Er moet dan een nieuw beschermingsschema aangemaakt worden en alle back-ups dienen opnieuw gestart te worden.**

De toegang tot de Acronis Cyber Protect web-interface is beveiligd met tweefactorauthenticatie en een gebruikersnaam en wachtwoord login. U kunt de tweefactorauthenticatie uitschakelen, maar dit wordt ten strengste afgeraden in verband met de veiligheid.

Ondersteunende medewerkers van KPN werken volgens stringente eisen:
- Versleutelde gegevens zijn niet toegankelijk.
- Er worden strenge procedures gehanteerd bij de afwikkeling van ondersteuningsaanvragen.

Om aan deze standaarden te voldoen, worden jaarlijks alle platforms en procedures binnen KPN EEN MKB onderworpen aan een strenge audit door een extern adviesbureau.

# 2 Technische specificaties

## 2.1 Randvoorwaarden voor het gebruik van de oplossing

Er is een internetverbinding noodzakelijk met een minimale uploadsnelheid van 1 Mbit/s. Als er een firewall gebruikt wordt, dan dient een aantal poorten open te staan om met het Acronis Cyber Protect Platform te kunnen communiceren en om clients en updates te kunnen distribueren. Hoe u deze poorten kunt openstellen, vindt u hier (vanaf Stap 5).

Voor Cyber Protect-functies is Microsoft Visual C++ 2017 Redistributable vereist. Tijdens de installatie van Acronis Cyber Protect wordt automatisch gecontroleerd of dit op uw machine(s) is geïnstalleerd. Als dit niet het geval is, wordt u gevraagd dit te installeren.

Er is vrije schijfruimte vereist om de Acronis-agent te installeren. Hoeveel ruimte u nodig heeft, vindt u hier.

## 2.2 Softwarevereisten

### 2.2.1 Besturingssystemen en overige omgevingen

Een compleet overzicht vindt u hier.

### 2.2.2 Ondersteunde virtualisatieplatforms

Een compleet overzicht vindt u hier.

### 2.2.3 Microsoft SQL Server, Exchange Server, Sharepoint, overig

Een compleet overzicht vindt u hier.

## 2.3 Ondersteunde bestandssystemen

Een compleet overzicht vindt u hier.

## 2.4 Acronis-datacenterlocaties en certificeringen

Een compleet overzicht vindt u hier. De Acronis-datacenters in Duitsland worden gebruikt binnen de KPN EEN MKB Acronis Cyber Protect-oplossing.

## 2.5 Beschikbaarheid dienst en gepland onderhoud

Voor de dienst Acronis Cyber Protect wordt, ten aanzien van de continue levering, de volgende minimale beschikbaarheid gegarandeerd:

- 99,89% beschikbaarheid (back-up maken en herstellen) op maandbasis, maximaal 0,48 uur per maand niet beschikbaar.
- 99,89% beschikbaarheid (back-up maken en herstellen) op jaarbasis, maximaal 9,38 uur per jaar niet beschikbaar.

Het oplossen van incidenten en problemen waarbij de dienstverlening zelf wel beschikbaar blijft, wordt niet meegeteld in de tijd dat de dienst niet beschikbaar is. Het uitlopen van gepland onderhoud wordt wel meegeteld als tijd dat de dienst niet beschikbaar is. Als er sprake is van storingen waarop KPN geen invloed heeft, worden deze uitgesloten van de beschikbaarheid. Deze storingen kunnen zijn:

- Storingen op het internet/publieke netwerk.
- Storingen die worden veroorzaakt door componenten die niet vallen onder de dienstverlening en die niet vallen binnen verantwoordelijkheid van KPN.
- Storingen die worden veroorzaakt door misbruik van de dienstverlening door u of uw eindgebruikers.
- Calamiteiten zoals een (natuur)ramp of een niet-verwachte gebeurtenis die ernstige schade kan veroorzaken.

### 2.5.1 Maintenance Window

Gepland onderhoud vindt plaats binnen het Maintenance Window, op woensdag van 02.00 uur tot 07.00 uur. Normaal gesproken is de dienst door de redundante opbouw tijdens dit onderhoud normaal beschikbaar.

# 3 Service

## 3.1 Gebruikersvragen

Voor meer informatie over Acronis Cyber Protect kunt u terecht op kpn.com/cloudservice.

## 3.2 Communicatie vanuit KPN

Tijdens de aankoop van de dienst heeft u een e-mailadres opgegeven. Alle communicatie over bijvoorbeeld herstellen van het wachtwoord of factuur- en onderhoudsinformatie ontvangt u via het door u opgegeven e-mailadres.

## 3.3 Abonnement

De looptijd van uw abonnement is 1 maand. U kunt uw abonnement altijd naar boven of naar beneden bijstellen.

Op deze dienst zijn zowel de voorwaarden van Acronis als die van KPN van toepassing. De voorwaarden van Acronis vindt u hier. Vanuit KPN zijn de 'Algemene Leveringsvoorwaarden' en 'Aanvullende Voorwaarden Online Diensten' van toepassing. U vindt deze op kpn.com/allevoorwaarden bij 'Zakelijk' en vervolgens bij 'Algemene en Aanvullende Voorwaarden'. Tot slot is ook de 'KPN EEN MKB Dienstbeschrijving Algemeen' van toepassing. Deze vindt u op kpn.com/allevoorwaarden bij 'Zakelijk' en vervolgens bij 'KPN EEN MKB'.

## 3.4 Factuur

Voor Acronis Cyber Protect betaalt u een maandelijks tarief per gebruikersnaam. Facturering van de dienst gebeurt maandelijks per automatische incasso met 1 maand vooruitbetaling. Restitutie van abonnementsgelden bij opzegging is niet mogelijk.

## 3.5 Beveiligingsmaatregelen

U kunt zelf ook een belangrijke bijdrage leveren aan het beveiligen van uw informatiestromen en (elektronische) persoonsgegevens. Denk hierbij bijvoorbeeld aan het altijd gebruiken van tweefactorauthenticatie waar mogelijk, uw gebruikersnaam en wachtwoord regelmatig wijzigen of het (beter) beveiligen van uw interne draadloze netwerk.